IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

SECURITIES AND EXCHANGE COMMISSION, Plaintiff, v. SOLARWINDS CORP. and TIMOTHY G. BROWN, Defendants.	)	Civil Action No. 1:23-cv-09518-PAE **ORAL ARGUMENT REQUESTED**

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO EXCLUDE THE TESTIMONY OF MARK G. GRAFF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

RULES

OTHER AUTHORITIES

PRELIMINARY STATEMENT

Having failed to unearth facts in discovery to prove its claims, the SEC tries to salvage its case through its cybersecurity expert, Mark G. Graff, whom it retained to support its theory of "pervasive" cybersecurity failures. But Mr. Graff faces the same problem as the SEC: there is *no evidence* on which he can ground such an opinion. The result is an unreasoned, often incoherent effort to mimic the SEC's claims without any actual basis to validate them. Mr. Graff's testimony should be excluded under *Daubert* and Rule 702 for several reasons.

First, Mr. Graff's testimony does not "fit"—*i.e.*, is not sufficiently relevant to—the SEC's claims. The SEC alleges that SolarWinds *pervasively* failed to implement certain cybersecurity controls, but Mr. Graff admits he looked only at isolated events, and *did not analyze the frequency* of any purported lapses. Given this fundamental disconnect from the SEC's alleged theory, Mr. Graff's testimony is not relevant to the case and would only serve to confuse the jury.

Second, Mr. Graff's opinions should be excluded because they do not reflect any cybersecurity expertise. An expert in the field would assess SolarWinds' implementation of cybersecurity controls by reviewing policy documentation and artifacts generated from implementing those policies. But Mr. Graff instead simply looked at comments in emails and other non-technical documents and purports to divine what they mean. Jurors can interpret these statements for themselves, and Mr. Graff has no special ken to do so for them.

Third, Mr. Graff's opinions lack any indicia of reliability. His testimony is a muddle of inconsistent *ipse dixit*, rather than conclusions drawn from a reliable methodology. Indeed, Mr. Graff cannot even settle on what his opinions *are*, or coherently articulate what principles underlie them, without repeatedly contradicting himself and the SEC. His primary conclusion is that SolarWinds did not "consistently" adhere to the Security Statement—but he was unable to define that term and repeatedly admitted he did not evaluate the frequency of any supposed deficiencies.

He then shifts to a different opinion—that alleged lapses might have been few, but they were supposedly of such "magnitude" that they *could indicate* pervasive failures. That speculative, arbitrary inference is unsupported by any identified standard or methodology.

Finally, Mr. Graff repeatedly opines on what SolarWinds or its employees knew or should have known about alleged cybersecurity lapses. The law is clear, however, that experts are not permitted to testify about a defendant's knowledge or scienter.

For all these reasons, Mr. Graff's result-driven opinion should be precluded.

BACKGROUND[1]

A. SEC's Claims

The SEC's claims relate to SolarWinds' online "Security Statement," which gave customers basic information about cybersecurity controls the company implemented. The SEC challenges five discrete policies in the Security Statement (the "Subject Policies"), alleging they were false because SolarWinds supposedly suffered from "long-standing, pervasive, systemic, and material cybersecurity deficiencies" in each area. *See* Am. Compl. ("AC") ¶ 2.[2]

B. Mr. Graff's Opinions

The SEC retained Mr. Graff to offer expert opinions on SolarWinds' adherence to the Subject Policies. Mr. Graff was once the Chief Information Security Officer for NASDAQ OMX, a position he left nearly 10 years ago, and claims he has since operated a cybersecurity consulting company, while also serving as an adjunct professor at the University of Arkansas Little Rock. Ex. 3 (Graff Rep. ("GR")) ¶¶ 1, 5. Although Mr. Graff states he has "experience in evaluating the

[1] Citations to "Ex. __" refer to the exhibits attached to the concurrently filed Declaration of Serrin Turner in Support of Defendants' Motion for Summary Judgment. Citations to "DS __" refer to the concurrently filed Defendants' Statement of Undisputed Material Facts.

[2] *See also, e.g.*, *id.* ¶ 11 (alleging "*pervasive* cybersecurity problems"); *id.* ¶ 115 ("SolarWinds *pervasively* failed to follow an SDL during the Relevant Period") (emphasis added); *id.* ¶ 182 ("SolarWinds *routinely and pervasively* granted employees unnecessary 'admin' rights") (emphasis added).

cybersecurity practices of large organizations," *id.* ¶ 20, he admitted at his deposition that his consulting company has had a total of six clients in eight years, consisting of "small businesses" with 20 employees or fewer, and that he did cybersecurity assessments for perhaps "one or two" of them, which were "mostly informal," Ex. 50 (Graff Dep.) 7:5-8:12, 8:17-9:15.

Though Mr. Graff was engaged as a cybersecurity expert, he was not asked to—and did not—assess SolarWinds' cybersecurity practices as would a professional in the industry. Ex. 4 (Graff Rebuttal Rep. ("GRR")) ¶ 7 ("[M]y assignment was not to conduct [a cybersecurity] assessment."). That is, he did not look for documentation reflecting the Subject Policies and the day-to-day records generated from their routine implementation. Instead, Mr. Graff understood his assignment was to review "internal assessments, presentations, and communications" about SolarWinds' cybersecurity and to "evaluate, based on [his] experience, whether they depicted a state of cybersecurity consistent with the assertions in the Security Statement." Ex. 3 (GR) ¶ 45(d), *id.* ¶ 17. Mr. Graff did this by asking his "team" to run keyword searches across the many thousands of emails and other internal documents produced in this case—although Mr. Graff was unable to recall much about these keywords, or to explain whether he reviewed all documents responsive to them as opposed to only looking at those selected by his "team." Ex. 50 (Graff Dep.) 37:8-40:11.

Mr. Graff expressed his opinions in two reports—an opening Report dated October 25, 2024 and a Rebuttal Report dated January 24, 2025. Although Mr. Graff was asked to opine on SolarWinds' adherence to each of the Subject Policies, Ex. 3 (GR) ¶ 17, he did not endorse the SEC's theories on the NIST CSF or network monitoring.[3] His "main conclusion" is that "internal

[3] Mr. Graff stated that the Security Statement's representations on NIST CSF were "too vague for [him] to evaluate," Ex. 3 (GR) ¶ 21, and that he "found insufficient evidence either to evaluate SolarWinds' network monitoring practices," *id.* ¶ 24. The SEC has since told Defendants it does not intend to pursue its network monitoring allegations further. Apparently it is not ready to likewise abandon its NIST CSF allegations.

SolarWinds documents were inconsistent, from a cybersecurity perspective, with the Security Statement's representations" regarding role-based access controls, password requirements, and secure software development. Ex. 3 (GR) ¶ 23. His opinions are based on his interpretations of vague notations in scattered documents—the same ones cited in the Amended Complaint—as well as four specific "incidents" (as he calls them) that he recycles throughout his Report (*see infra* at 20).

As noted, the SEC's theory is that SolarWinds *pervasively* failed to implement the Security Statement in these areas. While Mr. Graff at times uses similar verbiage, he ultimately makes clear that he never actually evaluated or opines on the frequency of any lapses in SolarWinds' cybersecurity controls. *See, e.g.*, Ex. 4 (GRR) ¶ 15 ("[I have] never stated anything about the frequency of an issue."). Indeed, Mr. Graff concedes that no evidence of frequent failures exists, repeatedly testifying that SolarWinds implemented the Subject Policies as regular practice.[4]

Attempting to paper over this fundamental break from the SEC's pled theory, Mr. Graff introduces a different one. He states that, while the lapses he identified may have been infrequent, they were of such "magnitude" that they "suggest," or could "indicate," "systemic issues." *See, e.g.*, Ex. 3 (GR) ¶¶ 77-78, 84, 91-92, 93, 157, 179. Mr. Graff acknowledges, however, that "no organization has perfect cybersecurity and that any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed." Ex. 3 (GR)

[4] *See, e.g.*, Ex. 50 (Graff Dep.) 67:20-68:1-7 ("So in order to evaluate whether or not role-based access controls were in place in a manner that was consistent with this Security Statement, I took a look at what I could find about, how often, yes, they did it, and I think … that often, they did it correctly."), 151:19-152:4 (acknowledging that role-based access controls were implemented "as a routine practice"), 249:10-17 (acknowledging that password complexity appeared to be automatically enforced on a "majority" of SolarWinds systems), 143:21-144:2 ("There was some network monitoring that was being done, absolutely. There was a lot of it, from the appearances of it."), 269:6-11 ("I think they did vulnerability testing in many cases, probably most cases, in terms of product development."), 281:14-19 ("I think … that they conducted regression testing with some regularity."), 280:2-24 ("[M]ost of the time I think they did do penetration testing as it relates to products.").

¶ 101. And he does not identify any standard of "magnitude" allowing him to distinguish the issues he relies on from those "that any organization diligently assessing its cybersecurity will uncover, from time to time."

LEGAL STANDARD

Under Rule 702, an expert may offer opinion testimony only if:

> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue; (b) the testimony is based on sufficient facts or data; (c) the testimony is the product of reliable principles and methods; and (d) the expert's opinion reflects a reliable application of the principles and methods to the facts of the case.

FED. R. EVID. 702. "The first requirement under Rule 702 … 'goes primarily to relevance' or, as the Supreme Court has described it, 'fit' between the proffered opinion and the facts of the case." *City of Providence v. Bats Glob. Markets, Inc.*, 2022 WL 902402, at *8 (S.D.N.Y. Mar. 28, 2022) (quoting *Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579, 591 (1993)). The other three requirements ensure that "[i]n fulfilling its gatekeeping role, … the Court must also consider 'indicia of reliability.'" *Id.* (quoting *Amorgianos v. Nat'l R.R. Passenger Corp.*, 303 F.3d 256, 265 (2d Cir. 2002)). The "overarching subject" of Rule 702 "is the scientific validity and thus the evidentiary relevance and reliability of the principles that underlie a proposed submission." *In re Bear Stearns Cos. Sec., Deriv. & Erisa Litig.*, 2016 WL 4098385, at *2-3 (S.D.N.Y. July 25, 2016).

"*Daubert* and Rule 702 mandate the exclusion of" testimony that "is based on data, a methodology, or studies that are simply inadequate to support the conclusions reached," *Amorgianos*, 303 F.3d at 266, or that "is speculative or conjectural or based on assumptions that are 'so unrealistic and contradictory as to suggest bad faith.'" *Zerega Ave. Realty Corp. v. Hornbeck Offshore Transp., LLC*, 571 F.3d 206, 214 (2d Cir. 2009). The SEC bears the burden of satisfying Rule 702 by a preponderance of evidence. *City of Providence*, 2022 WL 902402, at *12.

ARGUMENT

I. Mr. Graff's Opinions Are Not Relevant

The theory the SEC has pled and must prove at trial is that SolarWinds suffered from pervasive cybersecurity failures with respect to the Subject Policies. However, by his own admission, Mr. Graff did not analyze the "frequency" of any purported failures by SolarWinds to implement the Subject Policies—which means he has no basis to opine about whether or to what extent any such failures were pervasive. His testimony is thus irrelevant, and should be excluded.

"For expert testimony to 'fit,' the testimony must have a valid 'connection to the pertinent inquiry' and be 'sufficiently tied to the facts of the case so that it will aid the jury in resolving a factual dispute.'" *Adesina v. Aladan Corp.*, 438 F. Supp. 2d 329, 342 (S.D.N.Y. 2006) (citation omitted); *see Daubert*, 509 U.S. at 597 (expert testimony must be "relevant to the task at hand"). Mr. Graff's opinions do not fit what the SEC must prove. The SEC alleges the Security Statement was misleading because SolarWinds suffered from "pervasive," "systemic," "persistent," and "routine" failures to implement the Subject Policies. *See, e.g.*, AC ¶¶ 2, 11, 115, 182. As the SEC put it: "This is *not a case about … isolated control failures*. Rather, the *widespread and persistent failure* to follow each of the [relevant] policies … was material." AC ¶ 233 (emphases added). And as a legal matter, policy statements like those in the Security Statement are not "false" unless there were pervasive failures to follow them. *See* Defs.' Mot. Summ. J. at 23. Liability thus turns on whether SolarWinds pervasively failed to implement the Subject Policies, and any expert testimony must fit that specific question. *See Koppell v. N.Y. State Bd. of Elections*, 97 F. Supp. 2d 477, 480 (S.D.N.Y. 2000).

Mr. Graff did not evaluate that issue. He specifically disclaimed doing so, stating in his Rebuttal Report: "[I have] never stated anything about the frequency of an issue." Ex. 4 (GRR) ¶ 15. Likewise, he testified, "I wasn't particularly interested in or searching for any kind of

frequency." Ex. 50 (Graff Dep.) 56:20-24, 57:2-15. This creates a disconnect from the SEC's required showing. To take one example, the SEC alleges that SolarWinds "frequently violated its own internal password policy," AC ¶ 326; but Mr. Graff admits he did not measure the frequency of any password policy violations, and that he has no evidence that such violations were a "frequent problem."[5] Likewise, the SEC alleges "SolarWinds routinely and pervasively granted employees unnecessary 'admin' rights," AC ¶ 182, yet Mr. Graff again admits he saw no such evidence.[6]

Mr. Graff's opinions therefore do not fit, let alone support, the SEC's theory that SolarWinds frequently failed to implement the Subject Policies. Accordingly, his opinions would not help resolve the pertinent inquiry, and should be excluded. *See, e.g.*, *Bats*, 2022 WL 902402, at *8, *10-11 (excluding expert testimony because "there is a clear disconnect between the facts of the case and Plaintiffs' theory of … liability, on the one hand, and [the expert's] data and the opinions they can reliably support, on the other"); *In re Elysium Health-ChromaDex Litig.*, 2022 WL 421135, at *30 (S.D.N.Y. Feb. 11, 2022) (excluding expert "testimony [that] is not relevant to the truth of" challenged statements); *In re Lyman Good Dietary Supplements Litig.*, 2019 WL 5682880, at *5 (S.D.N.Y. Oct. 31, 2019) (expert testimony "not 'tied to' … 'the primary issue in this case'" was "irrelevant, unhelpful, and ha[s] the potential to mislead or confuse"); *Malletier v. Dooney & Bourke, Inc.*, 525 F. Supp. 2d 558, 573 (S.D.N.Y. 2007) (excluding expert report for "lack of fit between the basic premise of the study" and plaintiff's "position in th[e] litigation").

[5] Ex. 50 (Graff Dep.) 259:4-9 ("Q. So you have no evidence that it was a frequent occurrence at SolarWinds to use noncomplex passwords? A. Frequent? I didn't really address frequency. … I don't think I have evidence that shows it was a frequent problem.").

[6] Ex. 50 (Graff Dep.) 159:22-160:9 ("Q. I'm asking you whether you've seen any evidence that SolarWinds routinely and pervasively granted employees unnecessary admin rights? A. I don't know – I don't know that I would characterize it as a routine failure."). As discussed *infra* § III.A., this admission also renders speculative and unreliable any opinions Mr. Graff proffers that SolarWinds did not "consistently" implement cybersecurity controls, or that the incidents he focuses on are "indicative of systemic issues."

II. Mr. Graff's Opinions Are Not Based on Any Special Expertise

"To constitute an expert witness, the testimony must be based on 'scientific, technical, or other specialized knowledge.'" *United States v. Scali*, 2018 WL 543584, at *3 (S.D.N.Y. Jan. 23, 2018) (citing FED. R. EVID. 702(a)). That is, "[t]estimony is properly characterized as 'expert' only if it concerns matters that the average juror is not capable of understanding on his or her own." *United States v. Mejia*, 545 F.3d 179, 194 (2d Cir. 2008). Nothing about Mr. Graff's analysis requires any specialized or technical expertise.

To start, consider what expertise *would be* helpful to evaluate the SEC's claims that SolarWinds pervasively failed to implement the controls described in the Security Statement. As explained by Defendants' expert Dr. Gregory Rattray (formerly the national Director of Cybersecurity and now a consultant, who, unlike Mr. Graff, regularly assesses large organizations' cybersecurity programs), a standard cybersecurity assessment would "examine *direct evidence* of the company's implementation of those controls—in the form of written policies describing the controls and day-to-day documentation generated from the operation of the controls." *See* Ex. 2 (Rattray Rep. ("RR")) ¶¶ 5, 17-22, 101. The expert would then determine if that direct evidence is consistent with what they would expect to see if the controls were in place. *Id. That* is the sort of evidence Dr. Rattray analyzed—*e.g.*, the artifacts routinely generated through the Company's access-provisioning processes, network monitoring, and software security testing—and it readily reflects that the Subject Policies were in place. *See, e.g.*, Ex. 2 (RR) ¶¶ 43-53, 94-98.[7]

Mr. Graff undertook no such analysis. He admits that "my assignment was not to conduct [a cybersecurity] assessment." Ex. 4 (GRR) ¶ 7. He did not focus on the documentary evidence of

[7] This straightforward methodology is of course not unique to cybersecurity. For example, if an accounting expert were to assess the accuracy of a company's financial statements, they would review the evidence underlying those statements—*e.g.*, the company's books and records, and its processes for tracking revenue and expenses. The expert would not conduct a keyword search of internal emails discussing finances. Even if such discussions could be understood without context, they are no substitute for primary source data.

the Company's day-to-day implementation of the Subject Policies. Not only does Mr. Graff barely mention such documentation in his Report, he deliberately excluded it from his analysis, stating, remarkably: "Even if I had found a large number of additional internal documents describing SolarWinds adhering to industry norms at times, these would not have changed my opinions." Ex. 3 (GR) ¶ 46. This is hardly how an expert in the field would operate: they would not ignore large volumes of documents evidencing compliance with the very practices being assessed. *See In re Mirena Ius Levonorgestrel-Related Prods. Liab. Litig. (No. II)*, 341 F. Supp. 3d 213, 242 (S.D.N.Y. 2018) ("Where an expert ignores evidence that is highly relevant to his conclusion, [but] contrary to his own stated methodology, exclusion of the expert's testimony is warranted."), *aff'd*, 982 F.3d 113 (2d Cir. 2020); *ECD Inv. Grp. v. Credit Suisse Int'l*, 2017 WL 3841872, at *13 (S.D.N.Y. Sept. 1, 2017) (excluding expert testimony where "[t]here appears to be no explanation … for why [the expert] would ignore [relevant] data that *was* before him").

Rather than analyzing such direct cybersecurity artifacts—which Mr. Graff might credibly claim to have special expertise in interpreting—Mr. Graff instead focuses on interpreting obscure language in emails and slide decks and purporting to divine whether the authors were stating something "inconsistent" with the Security Statement.[8] That is something a lawyer might do, not a cybersecurity expert. Mr. Graff has no specialized expertise in interpreting the intended meanings of emails or stray comments in PowerPoint slides—regardless of whether the documents generally relate to cybersecurity. *See, e.g.*, *Accent Delight Int'l Ltd. v. Sotheby's*, 2023 WL 2307179, at *28 (S.D.N.Y. Mar. 1, 2023) (excluding opinion that "merely rehashes evidence in the case without

[8] *See, e.g.*, Ex. 3 (GR) ¶ 45 (describing methodology as running keyword searches across internal documents produced in discovery and then deciding whether they are consistent with the Security Statement); *see also* Ex. 4 (GRR) ¶ 7 ("My methodology of reviewing SolarWinds' internal documents and emails was in line with my assignment."); Ex. 50 (Graff Dep.) 27:20-28:5 (stating that he looked for inconsistencies with the Security Statement "as expressed in the e-mails and the reports and the presentations and the other internal evidence").

providing any expert analysis, as when [expert] describes the contents of invoices and emails … [or] opines on the inferences to be drawn from such evidence"); *In re LIBOR-Based Fin. Instruments Antitrust Litig.*, 299 F. Supp. 3d 430, 490 (S.D.N.Y. 2018) (rejecting expert's "interpretation of trader communications" as not based on expertise, and noting the "concern is heightened" where expert "offers no explanation of how the communications that she reviewed were selected"); *LinkCo, Inc. v. Fujitsu Ltd.*, 2002 WL 1585551, at *2 (S.D.N.Y. July 16, 2002) (excluding report based on expert's review of "documents, … deposition transcripts and exhibits," because "testimony by fact witnesses familiar with those documents would be 'far more appropriate ... and renders [the expert's] secondhand knowledge unnecessary'"); *United States v. DynCorp Int'l LLC*, 715 F. Supp. 3d 45, 64 (D.D.C. 2024) (excluding opinion because a "jury is 'just as competent' as [the expert] to read the [cited] emails and presentations"); *Mid-State Fertilizer Co. v. Exch. Nat. Bank of Chi.*, 877 F.2d 1333, 1340 (7th Cir. 1989) (rejecting testimony because "[a]n economist could have developed a model" and compared it to the evidence, yet expert merely "examined materials produced in discovery and drew inferences from the record").

Daubert and Rule 702 do not permit Mr. Graff to tell the jury what he thinks was meant by remarks in internal communications—particularly when his interpretation is *contrary to what the authors themselves* explained they meant under oath.[9] To the extent the comments in these emails and other documents require additional context to understand—as they all do—it is not Mr. Graff's place (nor does he have any expertise) to tell the court or the jury what the authors meant to convey. *See In re Terrorist Attacks on Sept. 11, 2001*, 2024 WL 5077293, at *5 (S.D.N.Y. Dec. 11, 2024) (party may not "use an expert witness as a vehicle to summarize the relevant facts … and then opine—or, more accurately, argue—that its theory of the case is the correct one," which amounts

[9] *See* Ex. 2 (RR) ¶¶ 138, 141-43, 148-49, 153, 155, 162, 165, 211.

to "giving a summation from the witness stand" (cleaned up)). And to the extent the SEC contends the meanings are clear,[10] that is all the more reason why expert testimony is unnecessary. *See United States v. Escobar*, 462 F. App'x. 58, 62 (2d Cir. 2012) (expert may not testify to matters "well within the grasp of the average juror"); *In re Longtop Fin. Techs. Ltd. Sec. Litig.*, 32 F. Supp. 3d 453, 460 (S.D.N.Y. 2014) ("[A]n expert may not offer testimony that simply 'regurgitates what a party has told him' or constructs 'a factual narrative based on record evidence.'"); *Jensen v. Cablevision Sys. Corp.*, 372 F. Supp. 3d 95, 116-17 (E.D.N.Y. 2019) (excluding expert's analysis of "a collection of company emails" and "internal company presentations" as "speculation regarding the meaning of certain internal documents" and "only presented … for the purpose of repeating the [proponent]'s factual narrative").

Simply put, Mr. Graff's analysis requires no specialized knowledge. He simply mimics the SEC's Amended Complaint by cherry-picking notations from internal communications and applies his own gloss to them in an effort to support the SEC's allegations. That is not expert testimony. "[A]n expert who is qualified as to certain subjects is not for that reason permitted to serve as an all-purpose 'color commentator' on the evidence, nor 'interpret' the evidentiary record for the jury outside of the bounds of his expertise." *Joint Stock Co. Channel One Russia Worldwide v. Infomir LLC*, 2021 WL 4810266, at *16 (S.D.N.Y. Sept. 30, 2021); *see, e.g.*, *Kraft Foods Glob., Inc. v. United Egg Producers, Inc.*, 2023 WL 6248473, at *3 (N.D. Ill. Sept. 19, 2023) ("The jury can read the 'documents' for itself."); *Sullivan v. Alcatel-Lucent USA Inc.*, 2014 WL 3558690, at *5-*6 (N.D. Ill. July 17, 2014) (finding expert's opinions "merely gratuitous and hence improper" where "he simply reads and interprets documents" and "does not draw on any expert qualifications or experience"); *In re Rezulin Prods. Liab. Litig*, 309 F. Supp. 2d 531, 551 (S.D.N.Y. 2004)

[10] Indeed, the SEC itself argues that "[i]t is *for a jury* to determine whether to *credit the plain language* of contemporaneous documents." SEC Pre-Mot. Ltr. 2, ECF No. 162 (emphases added).

(excluding testimony because "the glosses that [the expert] interpolates into his narrative are simple inferences drawn from uncomplicated facts that serve only to buttress [the proponent's] theory of the case").

III. Mr. Graff's Opinions Are Not Based on Any Reliable Methodology

Assessing an expert's reliability requires "rigorous" scrutiny of the principles and methods behind their opinions. *Amorgianos*, 303 F.3d at 267. Courts may consider various factors, including: "whether there are standards" guiding the expert's methodology; "the context in which the expert developed her opinion (i.e., … expressly for purposes of testifying)"; and "whether she has unjustifiably extrapolated from an accepted premise to an unfounded conclusion." *In re Terrorist Attacks*, 2024 WL 5077293, at *4 (quote marks omitted). Rule 702 does not "set[] a lower standard for witnesses with 'technical or other specialized knowledge' than for scientists." *Restivo v. Hessemann*, 846 F.3d 547, 576 (2d Cir. 2017). Whatever their background, the expert must base their "opinion on sufficient facts or data," and explain how their "experience leads to the conclusion reached, why that experience is a sufficient basis for the opinion, and how that experience is reliably applied to the facts." *Veleron Holding, B.V. v. Morgan Stanley*, 117 F. Supp. 3d 404, 444 (S.D.N.Y. 2015). Courts exclude opinions that reflect "too great an analytical gap between the data and opinion proffered" or supported "only by the *ipse dixit* of the expert." *Gen. Elec. Co. v. Joiner*, 522 U.S. 136, 146 (1997). Mr. Graff's opinions rest on nothing more than *ipse dixit* and baseless speculation, and fall well short of reliability.

A. Mr. Graff Lacks Any Reliable Methodology for His Conclusion That SolarWinds Did Not "Consistently" Apply the Subject Policies

Mr. Graff's "main conclusion" is that the documents he reviewed "indicate that SolarWinds failed to consistently apply the cybersecurity practices described in the Security Statement," GR

¶ 48—an opinion he repeats in similar formulations throughout his Report.[11] Mr. Graff never explains, however, what he means by "consistently," nor does he identify any principled methodology he applied to arrive at that conclusion.

Mr. Graff's vagueness about the term "consistently" is critical, because there are two possible alternatives as to what Mr. Graff could mean. He could mean that SolarWinds consistently *failed* to apply the Subject Policies—*i.e.*, that such failures were *frequent* (*i.e.*, pervasive, systemic, etc.) as the Amended Complaint alleges. Or alternatively—and much differently—he could mean that SolarWinds did apply the Subject Policies generally, but not "consistently," *i.e.*, *not always*—in other words, that there were failures, but they were *infrequent*. The problem for Mr. Graff is that, if the first alternative is what he means, then he lapses into self-contradiction; and if the second alternative is what he means, then he lapses into irrelevance.

At times, Mr. Graff seems to suggest that his opinion *is* that SolarWinds frequently failed to implement the Subject Policies, as he makes various (unsupported) claims that he found evidence of "many" instances of such failures.[12] But Mr. Graff ultimately makes clear that he is not expressing this view: Again, he specifically disclaims having any opinion that SolarWinds frequently failed to follow the Subject Policies. *See supra* at 6. Moreover, Mr. Graff repeatedly conceded at his deposition that SolarWinds implemented the Subject Policies with "regularity," as a "routine practice," "most of the time," and so on. *See supra* n.4. So, Mr. Graff cannot opine that

[11] *See also id.* ¶ 25 ("SolarWinds' fail[ed] to consistently follow [the representations in] the Security Statement … ."), ¶ 27 ("By failing to apply the controls described in the Security Statement in a consistent manner … ."), ¶ 46 ("[I] conclude[d] that SolarWinds did not consistently implement the practices described in several assertions in the Security Statement.").

[12] Ex. 3 (GR) ¶ 46 ("I have found evidence of *many flaws* in SolarWinds' practices, and they are *sufficient in the aggregate* for me to conclude that SolarWinds did not consistently implement the practices described in several assertions in the Security Statement." (emphases added)), ¶ 100 ("I provided *many examples* of instances in which the practices that SolarWinds discussed in internal documents were inconsistent with the categorical assertions made in the Security Statement." (emphasis added)).

SolarWinds consistently failed to implement the Subject Policies without contradicting himself and the undisputed evidence in the case—which would be its own grounds for exclusion. *See Davidov v. Louisville Ladder Grp., LLC*, 2005 WL 486734, at *2 (S.D.N.Y. Mar. 1, 2005) (excluding testimony because expert's conclusions were "in conflict with the uncontradicted evidence in the case"), *aff'd*, 169 F. App'x 661 (2d Cir. 2006); *New York v. Solvent Chem. Co.*, 225 F. Supp. 2d 270, 288-89 (W.D.N.Y. 2002) (excluding testimony where expert "does not define 'reprocessing'" and, if term had plain meaning, "there is no evidence" that reprocessing occurred).

On the other hand, if all that Mr. Graff means to say is that he saw a number of examples of SolarWinds deviating from the Security Statement, but that he has no reason to believe they were frequent, then his opinion becomes irrelevant. The Amended Complaint makes clear the case is not about whether there were "isolated instances of an employee failing to adhere to a policy"; rather, the core allegation is that there were *pervasive* failures. Further, Mr. Graff acknowledges that "no organization has perfect cybersecurity and [] any organization diligently assessing its cybersecurity will uncover, from time to time, some issues needing to be addressed." Ex. 3 (GR) ¶ 101; *see* Ex. 50 (Graff Dep.) 61:20-62:1 (conceding that "[t]he mere fact that occasionally a problem occurs … doesn't by itself indicate that there's a systemic issue"). Thus, if his opinion is merely that SolarWinds occasionally did something "inconsistent" with the Subject Policies—*i.e.*, that implementation was not perfect—then it is of no significance. *See supra* at 11 (cases on "fit").

Caught between these two horns of a dilemma, Mr. Graff nowhere clarifies in his Report what he means by saying that SolarWinds did not "consistently" follow the Subject Policies. Likewise, at his deposition, he was unable to do so despite being repeatedly pressed for clarification, instead giving conflicting answers and refusing to commit to any of them:

- "Q. I'm just trying to understand what you mean by the words you're using. So 'consistently', what does 'consistently' mean? Does that mean 100 percent of the time?

A. If they do it consistently [it] means they do it with consistency. They do it as a—as a regular practice. Q. … So when you say 'consistently' you mean do something as a regular practice, fair? A. I don't know that I would define it quite that way … ." Ex. 50 (Graff Dep.) 29:8-25.

- "Q … [W]hen you say SolarWinds didn't do this consistently, are you saying that they did not do it as a regular practice? Is that what 'consistently' means? A. Gee, I don't know that I can define it as quite being equivalent to—to that phrase. It's certainly something—if you do consistently and you do as a matter of regular practice, that's one of the ways you can do it consistently, but there are many other ways you can do it consistently too." Ex. 50 (Graff Dep.) 31:16-32:1.
- "Q. So can you not define for me what you mean and the terms that you use for your conclusions? A. The best answer I can give you is that when I looked at the evidence, that I find that when there—[were] many significant exceptions and variations and mistakes as I see, then I conclude that they weren't doing it consistently." Ex. 50 (Graff Dep.) 32:2-10.
- "Q. And I just want to be clear, basically you're saying you found many examples of noncompliance, and based on that, your conclusion is that these practices weren't consistently followed? … [D]oes your conclusion depend on your finding that there were many examples of noncompliance? A. I wouldn't say my conclusion depends on my finding." Ex. 50 (Graff Dep.) 32:21-33:6.

The reason for Mr. Graff's vacillation is obvious: If doing something "consistently" means doing it "as a regular practice," then he would have to concede that SolarWinds "consistently" followed the Subject Policies, as he concedes that it followed them as a regular practice. Alternatively, if his opinion that SolarWinds did not "consistently" follow the Subject Practices rests on how "many" supposed deviations he found, then that would amount to a claim about the frequency of those deviations, which Mr. Graff says he does not have any opinion about.

Mr. Graff's inability to even articulate a definition of "consistently"—the critical operative term in his "main conclusion"—renders his opinion unreliable. Without any clarity on that, it is impossible to understand what Mr. Graff is even trying to say, let alone what reliable methodology justifies him saying it. What is left is a purported conclusion about SolarWinds' practices that vaguely sounds bad, but has no real meaning—a classic example of unreliable expert opinion that would serve only to confuse rather than illuminate the facts. *See Pretter v. Metro N. Commuter*

R.R. Co., 206 F. Supp. 2d 601, 603 (S.D.N.Y. 2002) (excluding expert opinion relying on unexplained terms "sufficient" and "consistent" because "in its stated form the opinion is so vague as to be meaningless"); *Edwards v. Shanley*, 580 F. App'x 816, 824 (11th Cir. 2014) (affirming exclusion of testimony because expert "failed to explain what he meant by the use of the term 'prolonged'" and avoided specifics in deposition); *see also SEC v. Lek Sec. Corp.*, 370 F. Supp. 3d 384, 416 (S.D.N.Y. 2019) (precluding testimony where expert "fail[ed] to define" key terms and "[a]t times, … contradict[ed] himself" in his use of his own terminology); *In re LIBOR*, 299 F. Supp. 3d at 480 (unreliable methodology not saved by "terminological slipperiness" and "attempt to obfuscate … by shifting the definition of" key term); *LVL XIII Brands, Inc. v. Louis Vuitton Malletier S.A.*, 209 F. Supp. 3d 612, 647 (S.D.N.Y. 2016) (Engelmayer, J.) (precluding testimony where "the Court is left with no meaningful guidance as to how [the expert] reached his conclusion"), *aff'd*, 720 F. App'x 24 (2d Cir. 2017).

B. Mr. Graff Lacks Any Reliable Methodology for His Conclusion That Incidents of a Certain "Magnitude" Are "Indicative of Systemic Issues"

Mr. Graff tries to find a way out of the above dilemma by reframing his opinion as being about the "magnitude" of the deficiencies he claims to have found, rather than their frequency. He opines that, even though these purported lapses may have been few, they were supposedly of such "magnitude" that they are "indicative of systemic issues." Ex. 3 (GR) ¶ 157; *see also* Ex. 4 (GRR) ¶ 15 ("[T]he types of major issues that slipped through SolarWinds' internal controls need not materialize many times for them to indicate a systemic problem."); *id.* ¶ 47 ("Even if the incident materialized only once, the fact that an incident of this magnitude could develop indicates a systemic failure of internal controls."); Ex. 50 (Graff Dep.) 62:2-10 ("A significant issue … can indicate a systemic issue."). Mr. Graff's methodology here is not only unexplained, it is transparent nonsense.

Even if Mr. Graff had any discernible method for assessing the "magnitude" of the incidents he discusses—and he does not—the "magnitude" of a single incident has nothing to do with how "systemic" the underlying conduct is. By definition, calling an issue "systemic" means that it "affect[s] the whole of a system, organization, etc. rather than just some parts of it."[13] Accordingly, "[a] systemic problem cannot be shown by pointing to isolated incidents." *Wallace v. Jeffreys*, 2023 WL 2138337, at *18 (S.D. Ill. Feb. 21, 2023); *see Kang v. PayPal Holdings, Inc.*, 620 F. Supp. 3d 884, 899 n.2 (N.D. Cal. 2022) (holding that "violations would need to be frequent or widespread" to establish falsity, because "statements of compliance here did not 'reasonably suggest that there would be no violations"). A problem must occur *frequently* across a system in order for it to be "systemic"; and the occurrence of a single incident, no matter how significant it might be, does not imply anything about how often similar incidents occur. As Defendants' expert quipped in his report: "Aaron Judge made an error in this year's World Series that cost the Yankees the final game; that was a momentous mistake, but it hardly means he is a bad baseball player. (In fact, it was his first error of the year.)." Ex. 2 (RR) ¶ 106.[14]

Moreover, Mr. Graff does not even attempt to offer any "methodology" by which he purports to assess the "magnitude" of the "incidents" he discusses in his report. He merely identifies a few instances in which SolarWinds identified a risk that needed to be mitigated, and then proceeds to summarily characterize these "incidents" as "significant," "major," or "potentially catastrophic." *See, e.g.*, Ex. 3 (GR) ¶¶ 52, 73, 77, 155. Nowhere does he identify any scale of

[13] *See Systemic*, Cambridge US English Dictionary, http://bit.ly/syst01 (last visited Apr. 25, 2025).

[14] Mr. Graff does not make clear what he even means by "systemic issues" or that he even believes SolarWinds in fact had such issues. Instead, he seems to hedge his bets by asserting that certain events are "*indicative* of systemic issues." *See, e.g.*, Ex. 3 (GR) ¶ 77 ("The fact that such major events slipped through the cracks is indicative of systemic issues."), ¶ 92 (stating, as to a particular incident, that it is "suggestive to me of systemic problems"); Ex. 4 (GRR) ¶ 7 ("[T]he gravity of these incidents indicates a systemic issue."). This inability to state a clear conclusion only further underscores Mr. Graff's lack of any reliable methodology.

"magnitude" recognized in the field that justifies these characterizations. Nor does he explain how the issues he focuses on are any different from the sorts of "issues needing to be addressed" that Mr. Graff says "any organization diligently assessing its cybersecurity will uncover[] from time to time." Ex. 3 (GR) ¶ 101. Instead, Mr. Graff just makes the *ipse dixit* assertion that the issues he highlights "do not constitute the kind of routine minor problems that a company would encounter if it followed security best practices and industry norms in the manner described in the Security Statement," Ex. 3 (GR) ¶ 25. The "subjectivity and vagueness" of this conclusion is incompatible with any reliable methodology. *See Almeciga v. Ctr. for Investigative Reporting, Inc.*, 185 F. Supp. 3d 401, 425 (S.D.N.Y. 2016) (excluding testimony on similar basis). Moreover, the conclusion contradicts Mr. Graff's repeated admissions that SolarWinds *did* routinely follow the practices "described in the Security Statement." *See supra* n.4; *see also In re Fed. Home Loan Mortg. Corp. (Freddie Mac) Sec. Litig.*, 281 F.R.D. 174, 181 (S.D.N.Y. 2012) (concluding that expert's "internally inconsistent" analysis was "unreliable").

An example helps to illustrate the vapidity of Mr. Graff's analysis. Mr. Graff cites an email chain he says shows that "certain developers had unnecessary access to a dataset," specifically, a dataset of customer billing data. Ex. 3 (GR) ¶¶ 79-85 (citing Ex. 29 (SW-SEC00254254)). However, the email chain merely reflects that certain SolarWinds engineers were "improving [SolarWinds'] billing system," and that, to complete that project, they needed to pull live billing data from the system for testing. *See* Ex. 2 (RR) ¶¶ 121-126; Ex. 29 (SW-SEC00254254). To access that data, the developers had borrowed the login credentials of a different employee with "SuperUser" access, which was the type of access needed to pull the data. Borrowing another user's credentials was flagged as a security violation, leading the developers to request "SuperUser" access for themselves. The request was evaluated by the InfoSec team, including Tim

Brown. While "SuperUser" access came with both "read" and "write" permissions, and the engineers only needed to read the data for their project, there was not an existing "read-only" level of access built into the system as an available option, and creating one would require significant engineering work. Because the billing system project was considered high-priority, the decision was made to grant the developers in question SuperUser access to the system so they could complete the project, and in the meantime engineering work would be done to create a read-only level of access for future use. Mr. Brown specifically accepted this decision as "Low" risk. *See* Ex. 2 (RR) ¶¶ 123; Ex. 50 (Graff Dep.) 170:3-10.

Mr. Graff inexplicably argues that "a problem of this magnitude" implies that "practices were not in place" to ensure that the Security Statement's representations about role-based access controls "were consistently implemented across the organization." Ex. 2 (RR) ¶ 84. This conclusion is unfounded for several reasons. First, granting these specific engineers access to this specific billing system was not a "problem" of significant "magnitude," nor was it "inconsistent" with the Security Statement's representations about role-based access controls. These developers *needed* access to billing data to complete their project, and the only way to give it to them at the time was to grant them SuperUser privileges on that system. In other words, the access was *necessary to perform their role*, as even Mr. Graff conceded at his deposition.[15] The only risks from granting that access (as opposed to a read-only form of access that did not exist) were the risk that the engineers might accidentally modify the data, or the highly remote risk they would intentionally modify it—risks that Mr. Brown understandably considered "low." As Dr. Rattray explains, Mr. Graff's attempt to puff up this episode as some kind of "major" incident is absurd:

[15] *See* Ex. 50 (Graff Dep.) 171:16-22 ("Q. … The principle [of role-based access] is employees getting access based on what they need to do for their role. Here there was a determination made that, in order to perform their role, they needed this access at the time. The company was entitled to make that determination, was it not? A. Yes.").

> While Mr. Graff strains to portray this and other issues as somehow akin to "not locking the front door" of a house, the analogy is not remotely apt. The situation here would be more analogous to giving a small set of trusted employees access to a file cabinet containing billing records—which they needed to view to do their job—with the risk being that they might spill coffee on the records while reviewing them or, in some farfetched scenario, that they might alter them for malicious purposes. While ideally it would be preferable set up a special room where they were not allowed to bring in coffee or a pen, the risk of simply allowing them to access the file cabinet directly would be low, and it would be reasonable for the business to accept that risk in order to get the work done. That is all that happened here.

Ex. 2 (RR) ¶ 125.

But even putting the non-existent "magnitude" of this "incident" aside, Mr. Graff fails to explain how this single episode is supposed to be "indicative of systemic issues" with role-based access controls across the Company. This was obviously a context-specific issue involving a few specific engineers who needed administrative access to a specific system for a specific project. It does not suggest that SolarWinds had some "systemic" practice of giving users at the Company administrative rights. Mr. Graff admitted as much at his deposition:

> Q. … [A]m I right, that in this case, we're talking about a single group of developers getting access to a single system?
>
> A. Yes ….
>
> Q. Okay. So … you're not contending that this shows that SolarWinds just pervasively granted everybody read/write access to all their systems; this was a single exception related to a particular team and a particular system?
>
> A. This particular incident, yes.

Ex. 50 (Graff Dep.) 173:18-174:14.

The same goes for the other "incidents" that Mr. Graff relies on—they are all limited to specific contexts, and Mr. Graff provides no explanation of how they are somehow "indicative of systemic issues." There are actually only three other "incidents" that Mr. Graff examines in any depth; he simply recycles them over and over in his Report. Briefly:

- **MSP Customer Support Remote Access to Customer Systems.** Mr. Graff cites a project SolarWinds undertook during the Relevant Period to limit the

access that customer support staff in the Company's managed service provider (MSP) business line had to customer environments. *See* Ex. 3 (GR) ¶¶ 67-74, 186-88 (citing Ex. 32 (SW-SEC00631418)). Those personnel needed the ability to remotely access customer environments when customers requested support, but SolarWinds determined that the remote access should be read-only by default; so it undertook an engineering project to build that limitation into its in-house MSP customer-support platforms. As Mr. Graff acknowledged at his deposition, this issue, too, concerned the access that "a particular set of employees had … within a particular system" and did not provide any basis to conclude "that SolarWinds' employees generally had excessive access."[16] Moreover, while Mr. Graff labeled this incident "potentially catastrophic" because of the risk of an employee abusing access to customer environments, no such abuse ever happened, and the point of the project was to minimize that risk before it ever materialized. Thus, as Mr. Graff acknowledged, this "incident" showed SolarWinds identifying and remediating a risk, similar to what he would expect to see in any good cybersecurity program as part of their efforts at continuous improvement.[17]

- **"solarwinds123" Password.** Mr. Graff cites the fact that, during the Relevant Period, SolarWinds' security team discovered that an account the Company maintained on a third-party server had a non-complex password—"solarwinds123"—and that the password had accidentally been included in a publicly searchable code repository as a result of an intern's error. *See* Ex. 3 (GR) ¶¶ 86-93, 128-33. Mr. Graff labels this a "major" event based on an erroneous belief that, if a hacker had discovered the password, they could have used the account to disseminate malicious software to customers. Ex. 3 (GR) ¶ 87.[18] In any event, he admitted the password was for a single account out of many thousands used by the Company, and that had no basis to believe that the use of non-complex passwords was "a frequent problem." *See* Ex. 50 (Graff Dep.) 259:4-9.

- **Security Testing of OIP.** Mr. Graff also spends many pages in his report faulting SolarWinds for not doing security testing of an internal business

[16] Graff Dep. 178:17-24 ("Q. So, again, I just want to be clear on what we're talking about. You're not arguing from this document that SolarWinds' employees generally had excessive access; you just pointed to this as an instance where a particular set of employees had more access than they needed within a particular system? A. I think that's right.")

[17] Ex. 50 (Graff Dep.) 183:18-24 ("Now, just generally though, isn't this what a good cybersecurity program is supposed to do, when risks arise, take steps to mitigate them? A. Right. Q. And, again, the security statement doesn't say anywhere that SolarWinds' access controls were perfect? A. That's true."), 186:15-19 ("There's all sorts of risks that can be identified from time to time; that's what happens in [a] cybersecurity program, right? A. Sure, and there are incidents like this one [*i.e.*, the MSP customer support issue] that happen that will trigger analysis and improvements.").

[18] In fact, the account could not have been used to replace SolarWinds files with malicious files on SolarWinds' download site. *See* DS ¶¶ 114-16. Mr. Graff admitted at his deposition that this would change his assessment of the incident. Ex. 50 (Graff Dep.) 263:20-264:11.

> application known as Orion Improvement Program or "OIP" before June 2020 (when the Company did so in investigating whether the OIP server was under attack, which it turned out not to be). *See* Ex. 3 (GR) ¶¶ 168-83. This "incident" is a non-issue to begin with: The Security Statement only represents that SolarWinds did security testing of its "products," and Mr. Graff acknowledged at his deposition that OIP "was not a product." *See* Defs.' Mot. Summ. J. at 38; Ex. 50 (Graff Dep.) 290:7-12. Moreover, Mr. Graff does not even claim that the lack of testing of OIP somehow indicates that SolarWinds systemically failed to do security testing of its actual products. Again, he admitted that SolarWinds routinely performed the product security testing described in the Security Statement. Ex. 50 (Graff Dep.) 269:1-271:20, 280:25-281:19.

The foregoing constitutes the core body of "evidence" Mr. Graff cites for his conclusion that SolarWinds suffered "incidents" of serious "magnitude" that are "indicative of systemic issues." It is evident there is no "methodology" at work here, let alone a rigorous one. Instead, after searching through the tens of thousands of documents SolarWinds produced to the SEC, Mr. Graff found a few isolated issues SolarWinds addressed during the Relevant Period, which he throws into a hat he arbitrarily labels "major incidents," waves a magic wand, and then attempts to pull out a rabbit he calls "systemic issues." Mr. Graff is simply trying to mimic the SEC's allegations that SolarWinds suffered from "pervasive" and "systemic" cybersecurity deficiencies, without having any data or doing any analysis that would permit such a conclusion. *See Bats*, 2022 WL 902402, at *10 (finding there was "simply too great an analytical gap between the data and the opinion proffered," and that "[the expert's] efforts to plug the gap with his own '*ipse dixit*' do not suffice"); *In re LIBOR*, 299 F. Supp. 3d at 502 (excluding opinion based on expert's "review [of] various [internal] communications" and application of his "vast experience and knowledge gained through his work in the" industry, because "[s]uch a vague methodology is not a methodology at all"); *In re Mirena IUD Prods. Liab. Litig.*, 169 F. Supp. 3d 396, 486 (S.D.N.Y. 2016) (precluding testimony where the expert "does not seem to be basing her opinions … on any objective factors," such that the court was merely "left with a vague notion that in her personal opinion [the defendant's] conduct was inadequate"); *Faulkner v. Arista Records LLC*, 46 F. Supp.

3d 365, 381 (S.D.N.Y. 2014) ("[M]ethodology … aimed at achieving one result … is unreliable, and … must be excluded.").

Perhaps the most telling indicator of Mr. Graff's lack of any reliable "methodology" is that, at his deposition, his reasoning was turned against *his own* statements, and he reached a much different conclusion—conceding that a major incident that happened on his watch at NASDAQ did *not* imply any systemic failure to implement controls or contradict Mr. Graff's representations that such controls were in place. Specifically, while CISO at NASDAQ, Mr. Graff gave sworn congressional testimony that NASDAQ had implemented "[b]usiness continuity plans" that were "robust" and that "took into consideration real-time failovers of our market trading platforms"—*i.e.*, that NASDAQ had controls in place to seamlessly switch to backup trading systems if its primary systems failed. Ex. 44 (Graff Congressional Testimony) at 2; Ex. 50 (Graff Dep.) 79:10-81:13. Such failover controls were critical to the operation of NASDAQ—and the stability of the markets—in the event of a disruption of its systems. Ex. 50 (Graff Dep.) 81:24-83:6. However, after Mr. Graff's congressional testimony, those controls failed when a flaw in NASDAQ's systems prevented a failover from happening—bringing the exchange to a standstill for more than three hours. Ex. 18 (NASDAQ Press Release) at 2; Ex. 50 (Graff Dep.) 85:15-87:1. In other words, the "robust" business continuity controls Mr. Graff had represented were in place did not, in this instance, failover in real time as Mr. Graff had said they were designed to do. Ex. 50 (Graff Dep.) 90:5-6 ("Clearly, the business continuity plan didn't operate the way it should have.").

In contrast to the types of minor issues that Mr. Graff focuses on in his Report—which SolarWinds remediated *before* they resulted in any harmful incident—the NASDAQ failure was indisputably "major." Dubbed the "2013 Flash Freeze," it halted trading on NASDAQ for nearly half a day as traders waited for the problem to be fixed. The SEC Chair issued a press release about

the outage, emphasizing that it was a "serious" disruption to the markets that called attention to the importance of "addressing technological vulnerabilities of exchanges." Ex. 5 (SEC Press Release). As Mr. Graff acknowledged, "I think we can call that a major incident." Ex. 50 (Graff Dep.) 94:1-6; *see id.* at 95:22-96:2-8 ("[T]he disruption was certainly serious. The flaw in design … was, therefore, a serious flaw. … And so there's a – that's a serious issue as regards to the failovers, too."); *id.* at 96:15-97:8 ("It was a serious problem, I agree").

Nevertheless, according to Mr. Graff, this incident did not contravene his congressional testimony that NASDAQ had robust business continuity plans and failover systems in place:

> Q. Mr. Graff, you told Congress the business continuity plans were robust and took into consideration realtime failovers of market trading platforms. That was true, right? … That does not imply that there might not be serious issues that arise with respect to those controls?
>
> A. Well, we—yeah, I told Congress we had robust business continuity plans. We did. And the system, nevertheless, was overwhelmed and failed for a few hours in 2013.
>
> …
>
> Q. [NASDAQ's controls] were not perfect in that instance?
>
> A. They were not perfect, I agree.
>
> Q. And the consequences were major, right?
>
> A. Significant, you bet.
>
> Q. That doesn't mean NASDAQ didn't have business continuity controls in place?
>
> A. Yeah, we had controls in place. The controls seemed to have failed for a few hours, but yeah.

Ex. 50 (Graff Dep.) 97:23-99:5.[19] In other words, this incident, despite its unquestionable "magnitude," was apparently not "indicative of systemic issues" in Mr. Graff's view or "inconsistent" with his representations about NASDAQ's robust business continuity controls. That

[19] *See also id.* at 92:19-93:9 ("[W]hat I said in front of Congress was true. We did have the business continuity plans and some provisions that I felt were robust."), 91:2-16 (stating that he accurately represented to Congress the state of NASDAQ's business continuity controls notwithstanding that the systems were not perfect and a significant flaw manifested), 98:6-9 ("I told Congress we had robust business continuity plans. We did. And the system, nevertheless, was overwhelmed and failed for a few hours in 2013.").

Mr. Graff could reach such a radically different view in applying his "methodology" to his own past experience is a telltale sign that he has no "methodology" at all. *See Daniels-Feasel v. Forest Pharms., Inc.*, 2021 WL 4037820, at *17 (S.D.N.Y. Sept. 3, 2021) (excluding testimony because expert's "inconsistent application of the principles she claims to respect" revealed "[t]he unreliability of her methodology"), *aff'd*, 2023 WL 4837521 (2d Cir. July 28, 2023); *In re LIBOR*, 299 F. Supp. 3d at 478 n.23 (questioning "whether a single methodology, if applied inconsistently by an expert, could be properly termed a 'methodology' at all, let alone a reliable one.").

IV. Mr. Graff May Not Opine on Scienter

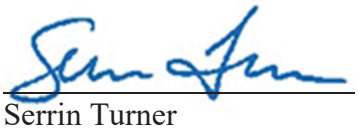
Finally, Mr. Graff's testimony should be excluded insofar as he purports to opine on who at the Company knew or should have known of certain cybersecurity deficiencies. He repeatedly states what he believes SolarWinds employees knew or should have known, in an attempt to shore up the SEC's scienter allegations. *See, e.g.*, Ex. 3 (GR) ¶ 28 ("The fact that such simple issues slipped through the company's internal systems should have alerted SolarWinds' cybersecurity leadership of potential systemic issues."); Ex. 4 (GRR) ¶ 2 ("I also concluded that significant deficiencies within these areas were known or made known to the relevant cybersecurity and leadership personnel" and "should have alerted SolarWinds' cybersecurity leadership that the Security Statement was inaccurately describing SolarWinds' cybersecurity posture."). However, testimony as to "the parties' states of mind … lie[s] outside the bounds of permissible expert testimony," as "[q]uestions about the parties' knowledge and intentions are classic questions of fact for the jury." *See Music Royalty Consulting, Inc. v. Reservoir Media Mgmt., Inc.*, 598 F. Supp. 3d 158, 194 (S.D.N.Y. 2022). Thus, beyond being inadmissible based on the problems with his opinions generally, Mr. Graff's opinions as to state of mind are excludable for this reason as well.

CONCLUSION

For the reasons stated, Mr. Graff's testimony should be excluded.

Dated: April 25, 2025

Respectfully submitted,



Serrin Turner
Matthew Valenti
Nicolas Luongo
LATHAM & WATKINS LLP
1271 Avenue of the Americas
New York, NY 10020
Telephone: (212) 906-1200
Facsimile: (212) 751-4864
serrin.turner@lw.com
matthew.valenti@lw.com
nicolas.luongo@lw.com

Sean M. Berkowitz (*pro hac vice*)
LATHAM & WATKINS LLP
330 N. Wabash, Suite 2800
Chicago, IL 60611
Telephone: (312) 876-7700
Facsimile: (617) 993-9767
sean.berkowitz@lw.com

Counsel for Defendants SolarWinds Corp. and Timothy G. Brown

CERTIFICATE OF SERVICE

I hereby certify that on April 25, 2025, I electronically filed the foregoing document with the Court via CM/ECF, which will automatically send notice and a copy of same to counsel of record via email.

Serrin Turner